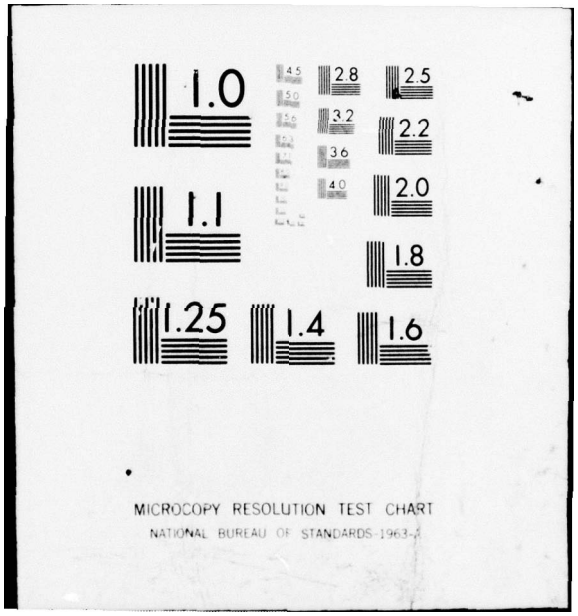
AD-A040 868 RAND CORP SANTA MONICA CALIF F/G 9/2
TESTIMONY BEFORE THE NATIONAL COMMISSION OF ELECTRONIC FUND TRA--ETC(U)
DEC 76 W H WARE
P-5767

UNCLASSIFIED NL

| OF |
AD
A040868

END

DATE
FILMED
7-77


1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
4.5
5.0
5.6
MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

6 TESTIMONY BEFORE THE NATIONAL COMMISSION OF ELECTRONIC FUND TRANSFERS,

10 WILLIS H. WARE

11 December 1976

12 12p.

14 P-5767

296600 Jmc

The Rand Corporation
Santa Monica, California 90406

TESTIMONY BEFORE THE NATIONAL COMMISSION OF ELECTRONIC FUND TRANSFERS

Mr. Chairman and Members of the Commission, it is certainly a privilege for me to be with you this morning. I imagine that each of you appreciates there is a certain sense of humor in my being at this table before you. Normally, in a fact-finding hearing of this kind I would be on the dais with you. I must say that it is lonely down here, but I suspect that it is good for my sense of humility and perspective.

My credentials for discussing security and privacy with you this morning include a lifetime career in computer technology, plus a personal and professional concern since the early 60s about the impact of that technology. As you have noted in your introduction, I was chairman of the Secretary's Special Advisory Committee on Automated Personal Data Systems, which, as you know, produced the definitive report, "Records, Computers and the Rights of Citizens"; and I am presently a member and Vice-Chairman of the Privacy Protection Study Commission. However, I do wish to make clear that I am expressing my personal views and convictions this morning. I am not speaking for the Commission nor am I expressing any position for the Corporation for which I happen to work.

From my discussion with your staff of what I might contribute to you, it was felt that an expository treatment of privacy and security matters would be helpful in your grappling with these fundamental aspects of EFT systems. So I would like to share with you my insights and personal convictions on such matters. What I would like to do is provide you with a broad framework and arguments that surround the two issues. With the time limitation, I will have to make some of my points as simple assertions and will not be able to defend them with a carefully detailed line of reasoning. I have supplied your staff with two papers* which I intended only as background and not as a substitute for my remarks this morning. I have not had time to send you written material, but I will provide it.

---

*P-5684, Privacy and Security Issues in Information Systems, The Rand Corporation, July 1976.

P-5685, Privacy Issues and the Private Sector, The Rand Corporation, July 1976.

The testimony before the Commission was given on October 27, 1976.

First of all, I think it is very important for your Commission to appreciate the time scale in which you should be examining the EFT matter. Until you finish your job and until your recommendations find their way into legislation or regulations or other actions, it will be three, perhaps as long as five years from now. If it turns out that our perception is somewhat deficient and that whatever legislation we put in place has shortcomings, it will be a few more years until such deficiencies appear and until we achieve remedial steps. I will argue that the time period on which your concern should be focused is roughly 4 to 8 years--perhaps 5 to 10--from now. While you must address the problems of tomorrow, there is a more serious set of the future that you must not overlook.

First, let me observe that the phrase "EFT system" is an ill-defined one. There are many such already in existence, a few of which you know include the automated clearing house, the cash terminal, and the point of sale terminal. Descriptive billing is a form of an EFT system; the national networks that are operated by organizations such as NBI* are EFT systems. Each deals with payment exchange, and therefore, funds exchange in one way or another; each represents an implementation that depends very critically on electronics and computer technology. In the broad sense, EFT systems are here now. Nonetheless, I would rather address my comments to what one might call "the fully developed environment" in which the merchant and his bank plus the customer and his bank are electronically linked to complete a transaction. Systems of this kind are just beginning to appear, but they will increasingly become more important.

The next order of business is to deal with three terms: confidentiality, security, and privacy. I will give you my best perception of the way the words are presently used and what they presently connote. Confidentiality is a status accorded to data or to information indicating that it is sensitive for some reason, and that it has to be both protected and controlled in dissemination. While there is an implication of control, there is not usually an iron clad agreement of control; there is an expectation on the part of the data subject that confidential material will be limited in its dissemination and used for stated purposes; sometimes there is a legal umbrella.

Security--and I am really addressing the term in the context of computer based systems--is the totality of safeguards required to do three things: first,

---

*National Bank Americard, Inc.

to protect computer based systems including its physical hardware, its personnel and its data against deliberate or accidental damage from some defined threat--a fire-bombed computer room is a major loss; second, to protect a system against denial of use by its rightful owners--one would not want the Fed-Wire or any automated clearing house to be captured by a dissident group and held hostage for a week or so; and third, to protect the data and the capabilities of the system against divulgence to or use by unauthorized persons--a stolen teller's manual could allow someone to browse through account records at an unattended terminal. Security is a protection concept, but please note that a part of security safeguards is the aspect of protecting against divulgence to unauthorized people as well as assuring divulgence only to authorized recipients.

Finally, privacy--a troublesome term because it is broad in scope. In the informational sense, which is really what we're all concerned about, privacy is the social expectation that an individual must be able to determine to what extent information about himself is communicated to or used by others; secondly, the social expectation that an individual will be protected against harm that might occur because of the information held about him in some record system; and third, the expectation that the individual will be protected against unwelcome or intrusive collection. For our purposes in this hearing, the third aspect is a minor one; the first two are the important ones. Thus, while security is largely a procedural and administrative matter implemented and supported, when necessary, by legislative or administrative arrangements.

The obvious problem in EFT systems is the unauthorized use of information by authorized recipients or by organizations holding it; and of course, that is the nub of the privacy concern. To the extent that existing legislation deals with privacy, it attempts to set norms for proper usage of information. The individual has an obvious stake in unauthorized use because it is there that he expects to exert his control over information about himself.

Now I would like to develop security and privacy as concepts. Depository and lending institutions certainly understand security in a classical sense in terms of locks, vaults, cameras, guards or alarms. Such precautions have evolved as a threat materialized; I doubt if your industry has ever done a system-wide threat analysis plus a conscious design of safeguards to counter the threat. Rather, protective mechanisms tend to be created and invented as the need warrants. I make this point because by contrast, an EFT system will be designed,

and will be implemented and installed as a system. It is quite unlike your conventional experience and the traditional way in which the financial industry has looked at security matters. I will argue that the organizations to be involved with the creation of any EFT system will have to decide what the threat against it is, and will have to very consciously select and implement the safeguards to counter the threat.

There are other important differences; let me use the bank vault as an example. The vault industry has implicitly estimated what the threat against a container is because the vault industry has decided on the wall thickness, on the kind of lock, and on the metallurgy of the steel. In terms of such decisions, it really has determined what the anticipated threat is. In fact, by testing, the bank vault industry can certify that a given container will withstand certain threats. As we all know though, vaults are breached either by circumventing the safeguards or subjecting them to a threat greater than the a priori perceived one. I make the point because in contrast, the computer industry simply does not have the long experience of the vault and safe manufacturers. The computer industry cannot deliver hardware and software systems that are certified against certain levels of attack. The industry is very much on the learning curve; but, there is a very broad and increasingly comprehensive set of safeguards that it can provide. In the end it becomes the responsibility of a depository-lending institution to perceive the threat against an EFT system and to select from the safeguards that the computer industry can give, the appropriate ones to array against the threat.

I would like to make a different point again on the security matter. A vault is in one place physically and it is under the control of a limited number of people. As we all know by now, any computerized system has tentacles throughout an organization. As EFT systems enlarge and expand, they will include remote terminals that are quite outside the control and surveillance of the institution's employees; the exposure of the system to outside people--the world--is higher. Furthermore, a substantial part of the threat against any automated system comes from the people within it; corresponding safeguards, of course, must be provided against them.

A final perspective on security. The technology that makes vaults strong--silent locks, tough steel, intricate alarms--is different from the technology

used to penetrate them--dynamite, plastic explosives, cutting torches, electronic snoopers, muscle power; in contrast, computer technology is on both sides of the fence. On one hand the computer is the device used to implement an EFT system or an automated management system, but another computer--even of the same kind--can also be used as a tool to attack the first. What is worse, the very operational capabilities that an organization will want in its system can be exploited by knowledgeable people to attack the system; for example, persistent probing might reveal functional anomalies that can be exploited by software changes surreptitiously made. In a real way, the computer with its capabilities can be turned against itself. I have made these points for perspective and to highlight the awareness that the classical and traditional view of how to do security must be thoroughly reconsidered in a computer era.

An aspect of security safeguards worth highlighting is that of auditing--a concept long familiar to the financial community. Traditionally, audits occur at periodic calendar intervals and depend on the availability of comprehensive records for effectiveness. Any "game playing" that may have been undertaken to probe the behavior of a manual system between audits will likely be undetected, even though knowledge of it could have suggested new precautions.

In an automated system, attempts to detect anomalous or exploitable aspects of it can take place sporadically in very short time intervals for each trial. It may well be that a system designed on the assumption that the operational world will always behave benignly as expected and will not notice such events. As part of security safeguards, internal continuous automated audits must be provided to detect and analyze attempts at penetration and unauthorized behavior by users of the system. The entire process of auditing and how it is implemented will need re-examination.

I will summarize the security issue in the following way. It is inevitable that any depository-lending institution will have to provide security safeguards. A management does not always notice that the computer system is as valuable to the business as the contents of the vault; if the currency is worth the vault, then the computerized system is worth its protection too. Security will have to be provided for your own assurance of performance and safety. However, please note that as automated systems enlarge into fully developed EFT ones, the security job will change; it will take on new and different

dimensions; the threat will have to be reevaluated and the safeguards restructured. Importantly, the entire concept of auditing must be looked at anew. While no one will argue that absolute security can be achieved, the appropriate point of view is that there presently exists a very extensive set of safeguards that can be employed against threats which can be defined. I would urge that when the Commission has hearings explicitly on the security matter, you get an appreciation from the vendors of what protections are available in hardware, software, communications, etc. I would especially urge that you get from the vendors an understanding of how such protections can fail. Furthermore, someone ought to describe the kind of threat that can be and has been mounted against computerized systems. From such discussions, you can have an awareness of what the present state of the whole matter is.

Turn now to privacy with its two aspects of concern: holding the individual safe from harm because of information about him in some record system, and giving him some measure of control over use of his information. To phrase it differently, the citizen wishes to be sure that decisions made about him are fair ones and he wants information about him used for purposes for which it was collected--he doesn't want it used for purposes to which he may object. As a social issue, informational privacy has arisen because modern public and private institutions inevitably require much information to conduct their business, and to run a large country whose people lead very complex lives. It has been discovered that information is a valuable commodity in a very real sense, and so organizations have fallen into the habit of using it for a wide variety of purposes, among others, of exchanging it with other institutions --all of it out of sight to the data subject in question. Many such uses, of course, are perfectly legitimate and socially acceptable. Many are onerous and distasteful when exposed to public view; there are many in the grey area, not wholly acceptable socially but, nevertheless, fulfilling in some people's minds a desirable purpose.

To me, privacy is an effort on the part of the country to seek a proper balance point between the genuine needs of an organization for information and the individual's concern for what is done with it.

Privacy is not concealing one's financial matters from a spouse; nor is it being annoyed if someone sits beside you in the airplane; nor is it resenting an intrusion into one's solitude. Rather, privacy reflects the emerging social expectation that information about one's self will be used--and I emphasize used--in ways that are socially acceptable, that are fair to the individual and that are constrained and controlled by law when necessary.

In the context of EFT systems, the personal information in question is the bank record. While I suspect that a detailed resolution may not yet have occurred, I would anticipate that the information captured by an EFT system would be construed as a bank record. I would note parenthetically that if the Bank Secrecy Act has caused your institutions to have cellars full of microfilm, in an EFT area it will cause your institutions to have warehouses full of magnetic tape. The usual bank record includes such things as amount on deposit, dates of deposit, dates on which checks were written or perhaps cleared, and payors of checks, but an EFT system will capture additional information. I remind you though that I am speaking of a fully developed environment in which merchant, customer and two banks are linked; I am not speaking of today's limited EFT environment. Among the extra things collected are the place, and the merchant name. If the "merchant" happens to be a large department store, it is likely to include the department name, and by inference, if not explicitly, one can know what has been purchased. A good system designer will almost surely record the date and time of each transaction so that the system can be audited and mistakes dealt with.

In a collective way, an EFT system can reveal a pattern of movement in a day, a pattern of purchases, habits of expenditure, preferred products or merchants, preferred charitable or religious causes, travel habits, or even transactions that members of a family are trying to conceal from one another. By virtue of the service that it provides, an EFT system inevitably and automatically captures much more information about an individual's daily affairs. I ask: what is to be the legal status of such a comprehensive record? Is it to be held in confidence and access to it legally controlled? Or will it be allowed to

become a body of valuable information about individuals that is open to browsing by interested or curious agencies of government? I mean that comment for federal, state and local level. Will it be open to private organizations for selective product solicitation, debt collection or political harassment? Interestingly, the EFT community does not stand alone. An airline reservation system or a lodging reservation system or even a credit card system captures information about the individual by virtue of the service that each gives, but an EFT system is unique in that it will have the most complete picture of an individual's life affairs. Therefore, it is important to realize that EFT records will inevitably become an attractive target of interest for exploitation by organizations of many kinds--public and private.

Let me put this in a different way. Take yourself aside from your positions here this morning as members of a Commission or as members of the depository-lending industry. Think of yourself as a member of society conducting your financial transactions on a daily basis in a fully developed EFT environment. Ask yourself--as I ask myself: Do you want access to such comprehensive personal information controlled or freely available for browsing? Do you have a personal expectation that such records will be used only for financial matters and not for exploitation in any manner of ways? Do you want government agencies--and I would especially note law enforcement or tax authorities--to have unconstrained access to such records? To have access not because you are suspect of a crime, but because your record happens to be one of a group that is being fished with the expectation of finding a clue to a crime that may have been committed or to some tax fraud that may have been perpetrated? Would you rather have some legal control so that access to your record is available only where there is a reasonable presumption that you have done wrong and the presumption has been argued before a judicial review before permitting access?

No matter how good security safeguards are, they will not be perfect. So I ask: Do you as an individual want to accept the risk that a dishonest or unscrupulous employee of a depository-lending institution will have access to and use information about some individual for a purpose of the employee's own? Are you as an individual really willing to take the risk that a comprehensive information system such as an EFTS can function with only the good will and good intentions of vested organizations to keep its behavior socially acceptable? Such are some of the questions that one has to struggle with in perceiving the privacy implications of an EFT world.

Now I would like to give an overall summary as follows. First, there are no essential technological obstructions to the forward progress of EFT systems; there is ample technology now available to do anything that an organization wishes to do, finds economically viable to do and is willing to pay for. Moreover, technology is advancing very fast. Second, EFT systems by their very nature will tend to capture more information than present automated versions do, which in turn capture more information than previous manual ones did. Third, an EFT system will create an information base that is bound to be of broad interest to other organizations. Fourth, things that have been hard to do will become easy. Manually it's difficult to find one record among hundreds of thousands, but in a computerized environment it is easy to select and find one record among hundreds of thousands or millions. Fifth, in regard to security, you will have to provide safeguards in your own interest as institutions--fraud, embezzlement and theft are real threats. Sixth, since EFT systems must deal with errors and mistakes, extensive means to monitor and audit them must be provided. Auditing, while a familiar function to financial institutions, will take on dramatically new dimensions in an EFT circumstance where records reside only in computers, some data may be transient and not permanently retained, and opportunities to tamper with the system are radically different. Finally, the social expectation now is that information about a person will be used in his best interest, will be used to make fair determinations about him, and will be used in ways that the individual and society collectively agree are acceptable.

I hope that I have been able to present the case for privacy and security convincingly. I tend to get wound up on this subject; but, if I have overreached my argument, I hope that I have not turned you off because I was turned on. From my perspective, I would not want you, a national Commission, to have a head-in-the-sand perspective, nor to deliberately elect to ignore the issues; I would regard that as a dereliction of your collective obligation to plan for and protect the future. If you are not convinced that privacy and security are crucial matter, it is my fault. If you're not convinced, I have not been able to provide you with sufficiently strong arguments, nor have I found a way to reach the responsive nerve. To guard against that possibility, I would leave you the standing option for me to provide additional material, written or verbal, and to work with your staff so that you will come to understand--as I have--the importance of privacy and the underlying technical

issue of security. I do appreciate the opportunity to have been invited to testify before you this morning; I will be glad to answer any questions that you may wish to ask.